

Blair L. Dawson, FIP, CIPP/US, CIPP/E, CIPM
Direct Dial: 312-642-6131
E-mail: bdawson@mcdonaldhopkins.com

January 23, 2023

VIA EMAIL (Idtheft@oag.state.md.us)

Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Toyotalift Northeast, LLC – Incident Notification

Dear Mr. Frosh:

McDonald Hopkins PLC represents Toyotalift Northeast, LLC (“Toyotalift”). I am writing to provide notification of an incident at Toyotalift that may affect the security of personal information of approximately 68 Maryland residents. Toyotalift’s investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Toyotalift does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Toyotalift recently learned that an unauthorized individual may have obtained access to their system between November 14, 2022 and November 22, 2022. Toyotalift immediately launched an investigation and analyze the affected system and files within. Toyotalift devoted considerable time and effort to determine what information was contained in the affected system. Based on its comprehensive investigation and document review, which concluded on December 27, 2022. Toyotalift discovered that the compromised system contained files with a limited amount of personal information including the affected residents’ full names and Social Security numbers.

To date, Toyotalift is not aware of any reports of identify fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Toyotalift wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Toyotalift is providing the affected residents with written notification of this incident commencing on or about January 24, 2023 in substantially the same form as the letter attached hereto. Toyotalift is offering the affected residents complimentary one-year memberships with a credit monitoring service. Toyotalift is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected

January 23, 2023

Page 2

residents are being advised to contact their financial institutions to inquire about steps to take to protect their accounts. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Toyotalift, protecting the privacy of personal information is a top priority. Toyotalift is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Toyotalift continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

If you have any additional questions, please contact me at (312) 642-6131 or bdawson@mcdonaldhopkins.com.

Very truly yours,



Blair L. Dawson, FIP, CIPP/US, CIPP/E, CIPM

Encl.



Return Mail to IDX:
10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code:

**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

Dear [REDACTED]

We are writing to inform you of a recent security incident affecting a portion of our stored electronic data. The privacy and security of the personal information belonging to our current and former employees is of the utmost importance to Toyotalift Northeast, LLC ("Toyotalift"). As such, we wanted to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

Toyotalift recently experienced a cybersecurity incident involving ransomware. Upon learning of this issue, we quickly contained the threat by disabling all unauthorized access to the network and immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to determine the extent of any compromise of the information on our network. Though our investigation is still ongoing, we do not have information indicating that your data has been misused. However, out of an abundance of caution we are notifying you of this incident.

What Information Was Involved?

The potentially acquired information included your personal information, specifically your full name and Social Security number.

What We Are Doing.

Upon learning of the issue, we commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals. After an extensive forensic investigation and manual email review, which was concluded on December 27, 2022 we discovered that the impacted server that was accessed contained some of your personal information. We have no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What You Can Do.

To protect you from potential misuse of your information, we are offering a **complimentary** one-year membership of credit and CyberScan monitoring through IDX. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Enrolling through IDX is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IDX's credit monitoring services including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against potential misuse of your information. The response line is available Monday through Friday 9 am – 9 pm Eastern Time.

Sincerely,

[REDACTED]
Toyotalift Northeast, LLC

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is April 24, 2023

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.